AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

Your Affiant, Marc Kudley, being duly sworn states that:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is offered in in support of an application for a search warrant to search the "**Target Accounts**" (described herein and more particularly described in Attachment

A) for (1) evidence of a crime, (2) contraband, fruits of crime, or other items illegally possessed, and (3) property designed for use, intended for use, or used in committing a crime (described herein and with greater particularity in Attachment B). In particular, this affidavit is made in support of an application under Rule 41(b)(1) and (b)(6)(A) of the Federal Rules of Criminal Procedure for a warrant to search for and seize evidence, instrumentalities, contraband, and fruits of violations of Title 21, United States Code, Section 841(a)(1), Distribution of controlled substances; Title 21, United States Code, Section 846, conspiracy or attempt to distribute controlled substances; Title 21, United States Code, Section 841(h)(1)(A), Distribution of controlled substances via the Internet; Title 21 United States Code, Section 952(a), Importation of controlled substances; Title 21, United States Code, Section 843(b), Illegal use of the mail and/or communication facility; and Title 18, United States Code, Section 1956, Money Laundering within the following user accounts:

a. User account "gregorian45" that is stored on the server hosting Tor hidden service Dream Market, a dark net marketplace identified by the Tor URL http://uhivlt5grrqjhad7.onion/?ai=1675,

b. User account "gregorian45" that is stored on the server hosting Tor hidden service Wall Street Market, a dark net marketplace identify by the Tor URL

http://wallst4qihu6lvsa.onion/signup?ref=276,

c. User account “steve1” that is stored on the server hosting Tor hidden service Point / T CHKA Free Market, a dark net marketplace identified by the Tor URL http://pointgg344ghbo2s.onion/auth/register/563636d36ab740e4720f44e8328441d3,

d. The coincure.net bitcoin wallet account associated with the email stevechase2015@protonmail.com or username “stevechase0702”,

e. The electrum.org bitcoin wallet account associated with the email stevechase2015@protonmail.com,

f. The bitstamp.net on-line bitcoin exchange account associated with the email stevechase2015@protonmail.com, client ID number 268962, or username Lanierlife9816,

g. The hitbtc.com on-line digital currency exchange account associated with the email lanierlife@gmail.com,

h. The paragoncoin.com on-line digital currency exchange account associated with the email lanierlife@gmail.com,

i. The gatehub.net on-line digital currency exchange account associated with the email lanierlife@gmail.com,

j. The bittrex.com on-line digital currency exchange account associated with the email lanierlife@gmail.com,

k. The localbitcoins.com on-line bitcoin exchange account associated with the username “davenport216” or email davenport1522@mail.com,

l. The binance.com on-line bitcoin exchange account associated with the username

"lanierlife" or email lanierlife@gmail.com,

m. The liqui.io on-line digital currency exchange account associated with the username "lanierlife" or email lanierlife@gmail.com,

(hereinafter, "**Target Accounts**"), as further described in Attachment A, which is appended to this affidavit and incorporated herein by reference.

2. Your Affiant is a United States Postal Inspector and has been so employed since May 2012, presently assigned at Cleveland, Ohio to investigate Prohibited Mailing offenses. I have received training in the detection and investigation of prohibited mailing offenses. I have worked U.S. Postal Service related investigations for approximately 6 years, during which time I have been the case agent for investigations leading to prosecution in U. S. District Court, as well as state courts.

3. As a Postal Inspector, I have also conducted online investigations, analyzed pen register and telephone toll data, analyzed financial records, executed controlled deliveries of controlled substances, interviewed witnesses, drafted and executed search warrants, seized illegal drugs and other evidence of drug violations in physical and electronic sources, processed seized evidence, assisted in online undercover purchases of controlled substances, and debriefed persons arrested and convicted of drug trafficking offenses regarding their illegal activity.

4. Through investigation and training, I have become familiar with the types and amounts of profits made by drug traffickers and the methods, language, and terms used to disguise their illegal activity. I know that persons engaged in drug trafficking require expedient forms of communication to maintain an adequate and consistent supply of drugs from sources, and to effectively market those drugs to customers. Individuals who buy and/or sell controlled substances on online marketplaces often rely on one or more means of

electronic communication (such as encrypted email and chat communications) as a means to facilitate this expedient communication.

5. Your Affiant knows based on training and experiences those individuals who traffic in one controlled substances such as Fentanyl and Carfentanil often traffic and possesses other controlled substances and controlled substances. Furthermore, based on my training and experience that individuals who engage in unlawful activity on the internet (including the dark net) sometimes also use the expertise that they learn to engage in other criminal activity online

6. Your Affiant knows based on training and experience that drug traffickers – particularly those using dark net marketplaces – often use parcel services that include, but are not limited to, U.S. Mail, FedEx, UPS, and DHL, to transport controlled substances. Your Affiant is further aware that dark net drug traffickers often use decoys (non-contraband items that can store narcotics and thus reduce the risk of detection) in their drug packaging. Use of these decoys sometimes costs the customer an additional fee.

7. Based upon my training and experience, Your Affiant knows that drugs are generally stored and dispersed at varied, and highly secret, locations to avoid seizure and theft.

8. In addition, Your Affiant is aware that drug distributors, particularly dark net distributors who have customers across the country and are not reliant on a local customer base, often travel for a variety of reasons, including to avoid law enforcement detection. They often use rental cars, flights, Ubers, and other means of transit to accomplish these goals. In addition, dark net drug traffickers also use hotels/motels or other forms of temporary stay as a base of operation while engaging in illegal activity.

9. Your Affiant is further aware that drug traffickers frequently launder drug

profits. In sophisticated drug trafficking enterprises, money is often laundered through corporate and personal accounts, both in the United States and abroad. Your Affiant is aware that records relating to these transactions are often found in electronic devices used by DTO conspirators and their associated businesses. This information is sometimes co-located in files or applications that also contain information regarding the legal banking information of their businesses, which usually play a role in the money laundering enterprise. These financial dealings are often done digitally through an electronic device. Furthermore, banks often provide information relating to financial transactions through automated texts or emails that are stored on electronic devices.

10. Your Affiant knows based on training and experiences those individuals who use the U.S. Postal Service or common carriers (e.g., FedEx) to traffic narcotics and narcotics proceeds/payments often possess U.S. Postal Service related receipts and mailing labels and have accounts with said services.

11. Your Affiant is aware that drug traffickers often maintain on hand at locations they occupy and/or control large amounts of U.S. currency as working capital to maintain and finance their narcotics activities and/or as profits derived from the sale of drugs. Similarly, when drug traffickers use virtual currencies such as Bitcoin, they often maintain virtual currency wallets at their home or on their person, or otherwise have those wallets accessible to them if they are stored online.

12. Your Affiant is further aware that drug traffickers frequently launder drug profits by purchasing assets. In sophisticated drug trafficking enterprises, real or sham businesses or real estate transactions are used to "clean" the proceeds of the drug operation. Drug traffickers often keep records of these transactions as a means of identifying the location of their illicit gain.

13. Your Affiant is aware that individuals involved in narcotics trafficking often

maintain records linking them to their trafficking activity and their drug trafficking associates. These records may be stored physically or digitally on internet sites such as Tor hidden networks, computers or other electronic devices or media. These records may include notes, records or ledgers of narcotics sales, debts owed, past or future shipments, and other records, including telephone records, which identify customers and/or other co-conspirators.

14. Based on Your Affiant's training and experience, Your Affiant is also aware that drug traffickers store on internet sites such as Tor hidden networks photos, videos, and other media associated with the sale, purchase, and distribution of illegal drugs. This media includes photographs and videos of the drugs and other items associated with their illegal activities to demonstrate their prowess and as an advertisement of their wares. These photos, videos, and other media often establish the identities of the individuals involved in the sale, purchase, and distribution of the illegal drugs.

15. Based upon Your Affiant's training and experience, Your Affiant knows that communication through electronic devices – such as through telephone calls, texts, chat, email, instant messaging, messaging over marketplaces on Tor hidden networks, and other applications – enables drug distributors to maintain constant contact with associates, drug suppliers, and customers. Your Affiant knows that it is common for drug trafficking organizations ("DTOs") to use these applications to communicate with associates relating to the logistics of their drug trafficking business and store information (purposely or inadvertently) relating to their unlawful activities.

16. Based upon my training and experience, Your Affiant is aware that drug traffickers also use internet sites such as Tor hidden networks for communication or other

forms of data storage or sending/receiving relating to bank records, account information, and other electronic financial records ties to the importation, transportation, ordering, purchasing, and distribution of controlled substances.

The facts set forth below are based upon your Affiant's personal knowledge learned through an investigation by the U.S. Postal Inspection Service, as well as information obtained from other federal, state, and local law enforcement and information obtained from additional sources. This Affidavit is being submitted for the purpose of obtaining a search warrant. Since this affidavit is being submitted for the limited purpose of establishing probable cause, Your Affiant has not included each and every fact known concerning this investigation.

17. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Section 841(a)(1), Distribution of controlled substances; Title 21, United States Code, Section 846, conspiracy or attempt to distribute controlled substances; Title 21, United States Code, Section 841(h)(1)(A), Distribution of controlled substances via the Internet; Title 21 United States Code, Section 952(a), Importation of controlled substances; Title 21, United States Code, Section 843(b), Illegal use of the mail and/or communication facility; and Title 18, United States Code, Section 1956, Money Laundering have been and continue to be committed. There is also probable cause to search the accounts listed herein, further described in Attachment A, for evidence, instrumentalities, contraband and fruits of these crimes as described in Attachment B.

JURISDICTION

18. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(A) because the facts herein establish there is probable cause to believe that the

district where the information is located has been concealed through technological means and that there is probable cause to believe that activities related to the crime being investigated occurred within this judicial district.

19. Federal Rule of Criminal Procedure Rule 41(b)(6) states, in relevant part:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means.

20. This warrant authorizes investigators to log into the **Target Accounts**, change the passwords on the accounts to prevent evidence tampering and protect the integrity of the seized information, and seize information described in Attachment B from the **Target Accounts**.

21. The servers that house the data contained in the **Target Accounts** are at an unknown location. The Dream Market, Wall Street Market, and Point / T CHKA Free Market are dark net marketplaces stored on the server hosting Tor network, a network design to conceal the locations of site administrators and to anonymize transactions. According to coincure.net, this entity is located in London, United Kingdom, but operate using a Tor network. The location of the servers for these entities is concealed through technological means. Your Affiant has identified business locations of the other digital currency wallet and digital currency exchange entities identified throughout this investigation, but the location of their respective servers is unknown.

22. According to electrum.org, this entity is located in Berlin, Germany. According to bitstamp.net, this entity is located in London, United Kingdom. According to hitbtc.com, this entity is located in New Territories, Hong Kong. According to

paragoncoin.com, this entity is located in Los Angeles, California. According to gatehub.net, this entity is located in London, United Kingdom. According to bittrex.com, this entity is located in Seattle, Washington. According to localbitcoins.com, this entity is located in Helsinki, Finland. According to binance.com, this entity is located in an unknown city in Malta. According to liquid.io, this entity is located in Kiev, Ukraine. The servers associated with these accounts are at unknown locations, but the accounts and data therein are accessible in the Northern District of Ohio. Investigators will execute the search by logging into the Target Accounts from computers located in the Northern District of Ohio and accessing the data.

23. The evidence summarized below establishes that the **Target Accounts** are directly tied to Elliet "E" Lanier's criminal scheme to obtain and distribute illegal narcotics via the dark net marketplace by using digital crypto-currency. The location of the information to be seized are either concealed through technological means or stored at unknown locations. The accounts are, however, accessible by any computer or electronic device with access to the Internet, including law enforcement devices within the Northern District of Ohio. This Court therefore has jurisdiction to issue the requested warrant.

BACKGROUND AND DEFINITIONS CONCERNING DARK NET AND CRYPTOCURRENCY INVESTIGATIONS

24. The "clear" or "surface" web is part of the internet accessible to anyone with a standard browser and that standard web search engines can index. The deep web is the part of the internet whose contents are not indexed by standard web search engines. The dark net is a part of the deep web that not only cannot be discovered through a traditional search engine, but also has been intentionally hidden and is inaccessible through standard browsers and methods.

25. The dark net is accessible only with specific software, configurations, and/or authorization, including non-standard communications protocols and ports, such as a Tor ("The Onion Router") browser. A Tor browser is designed specifically to facilitate anonymous communication over the internet. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle." Use of the Tor network bounces a user's encrypted communications through a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that Tor exit node IP address. A criminal suspect's use of Tor makes it extremely difficult for law enforcement agents to detect a host, administrator, or user actual IP address or physical location.

26. Dark net marketplaces operate on the dark net. These sites are generally only accessible through the input of specific addresses in a Tor browser. The dark net marketplaces function primarily as black markets, selling or brokering transactions involving drugs, cyber- arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the occasional sale of legal products. Dark net vendors (also known as distributors) operate on these dark net markets as sellers of these goods. They provide detailed information about

their wares on these sites, including listings of their drugs for sale, contact information (such as Tor-based email or encrypted messaging applications), and the prices and quantities of drugs for sale. Items purchased through dark net vendors are generally paid for in cryptocurrency such as Bitcoin. Cryptocurrency or virtual currency permits the anonymous exchange of unlimited amounts of digital currency to anyone in the world without the use of traditional banks or banking systems. Customers purchase these goods using a computer or smartphone.

27. Your Affiant is aware that some dark net marketplace vendors conduct the entirety of their transactions on the dark web marketplace. Other vendors use the sites as an advertising base and messaging system and conduct their financial business in peer-to-peer[1] transactions in order to avoid using third party escrow systems that they believe could be subject to law enforcement seizures as well as thefts, hacks, and scams.

28. Bitcoin (BTC) is a type of virtual currency, circulated over the internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency. Other currency includes Bitcoin Cash ("BCH"), Litecoins ("LTC"), Ethereum ("ETH" or "ether"), and Ripple (XRP). For ease of reference, the analysis below relating to Bitcoin generally applies to other types of cryptocurrencies (often collectively referred to as "Altcoins").

29. Bitcoin are sent to and received from BTC "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is

necessary to access the Bitcoin address. Only the holder of an address' private key can authorize any transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple BTC addresses at any given time and may use a unique Bitcoin address for each and every transaction.

30. To acquire bitcoin, a typical user purchases them from a virtual currency exchange. Your Affiant knows bitcoin can be referred to as virtual, digital, and/or cryptographic currency. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities.

31. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to- peer BTC network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflect any identifying information about either sender or recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

32. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can sometimes trace transactions to third party companies that collect identifying information about their customers and are responsive to legal process.

33. In addition to Bitcoin and other cryptocurrencies, there are also tokens. Like Bitcoin and Altcoins, tokens use blockchain technology. Tokens are digital assets that are powered through smart contracts. While tokens theoretically can be used to represent any assets that are fungible and tradeable, they are often used as a commodity similar in some ways to stocks or options. In these scenarios, tokens are created and distributed through an Initial Coin Offering (ICO). Through an ICO, a venture offers a stock of specialized crypto tokens for sale with the promise that those tokens will operate as the medium of exchange when accessing services on a digital platform developed by the venture. The sale of tokens provides capital to fund the initial development of the digital platform, although no commitment is made as to the price of future services (in tokens or otherwise). In this sense, tokens are a fungible and potentially highly volatile unit of value that can be easy to obtain. Your affiant is aware that dark net distributors are increasingly using tokens as a means of laundering their illicit gains.

34. Your affiant is aware that individuals conducting business in this manner must use a computer or other electronic device, such as a smartphone, tablet, or computer to conduct transactions involving cryptocurrencies or tokens. Users of cryptocurrencies or

tokens must establish electronic wallets to receive and send the bitcoin during these transactions. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, or computers. They may also be stored on third party wallet providers (such as Armory). Individuals often associate email accounts with these wallet providers and store information relating to that wallet on their email account. Your affiant is also aware that individuals conducting business by bitcoin can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. They are also often stored on email accounts, cloud or shared drives stored online (such as Google Drive), and other online storage mediums.

FACTS AND CIRCUMSTANCES REGARDING PROBABLE CAUSE

35. I know based on training and experience that U.S. mail is often used by narcotic traffickers to transport controlled substances. I know from my training and experience that the Priority Mail system is commonly used to transport controlled substances because Priority Mail provides traceability, reliability, and timely delivery. The guaranteed delivery timeframe of approximately two to three days for Priority Mail places time pressures on law enforcement agents to identify, search, and deliver these drug parcels in a timely manner.

36. On November 15, 2018, your Affiant was contacted by a Postal Inspector assigned to the USPIS Houston, Texas Field Office regarding an investigation involving the mailing of controlled substances from the Houston, Texas, area to various destinations throughout the United States. The USPIS Houston, Texas Field Office informed your

Affiant that the source of controlled substances in the Houston, Texas, area sells smaller quantities of controlled substances via the "dark web" marketplace in attempt to avoid detection from law enforcement.

37. The USPIS Houston, Texas Field Office informed your Affiant that on June 27, 2018, Postal Inspectors assigned to the USPIS Columbia, Maryland, Field Office intercepted USPS Priority Mail parcel bearing tracking number 9205 5901 7554 7700 0082 9085 44, addressed to Anthony Puglisi, 985 Saint Stephens Church Rd, Gambrills, MD 21054, with a return address of Smiths Candy Store, 990 Gillette St, Houston, TX 77019. Postal Inspectors executed a search of the parcel and identified blue round tablets marked as "A 215," purported to be Oxycodone Hydrochloride 30 milligram, a Schedule II controlled substance, concealed in a gold foil bag.

38. The tablets were submitted to the USPIS Forensic Laboratory for chemistry examination and were to found contain a detectable amount of Carfentanil, a Schedule II controlled substance. Based on the foregoing, investigators believe the source of the tablets disguised the tablets as Oxycodone Hydrochloride 30 milligram, but they actually contained Carfentanil.

39. The USPIS Houston, Texas, Field Office advised your Affiant that through an analysis of USPS business records, they identified a USPS Priority Mail parcel suspected of containing controlled substances that was mailed from the Houston, Texas, area to Cleveland, Ohio. Based on their knowledge of the investigation, the Postal Inspector assigned to the USPIS Houston, Texas, Field Office suspected that the USPS Priority Mail parcel destined for Cleveland, Ohio, originated from the same source of tablets that contained Carfentanil that was seized by Postal Inspectors from the USPIS Columbia,

Maryland, Field Office on June 27, 2018.

40. The parcel identified by the USPIS Houston, Texas, Field Office destined for Cleveland, Ohio, is described as USPS Priority Mail parcel bearing tracking no. 9205 5901 7554 7700 0111 5294 12, addressed to Steve Chase, 730 E 101st St, Cleveland, OH 44108, with a return address of Donald Candy Shop, 21441 Carrington Road, Houston, TX 77036 (hereinafter referred to as the "Target Parcel").

41. The Target Parcel is further described as a white USPS Priority Mail Flat Rate Envelope measuring approximately 12.5" X 9.5" in size and weighing approximately 3.5 ounces. The Target Parcel originated in Houston, Texas, on November 12, 2018, and was then processed by the USPS North Houston, Texas 77135 Processing Facility on November 14, 2018.

42. On November 16, 2018, your Affiant took possession of the Target Parcel after it arrived at the Cleveland, Ohio 44108 Post Office from the Cleveland, Ohio, Processing Facility, and transported it back to the USPIS Cleveland, Ohio, Field Office for further investigation. Your Affiant identified the Target Parcel as a suspect drug parcel based on several characteristics, including but not limited to type of mail, origin, destination, and size. The Target Parcel also listed a candy store as the sender, similar to the USPS Priority Mail parcel seized by Postal Inspectors assigned to the USPIS Columbia, Maryland Field Office in June 2018 that contained Carfentanil.

43. Your Affiant made inquiries with CLEAR, an electronic database that has proven reliable in previous investigations in determining the legitimacy of name, address, and phone number information, concerning the delivery address of 730 E 101st St, Cleveland, OH 44108, and was unable to identify an individual by the name of Steve Chase

at the address.

44. Your Affiant also conducted inquiries with CLEAR, concerning the return address of 21441 Carrington Road, Houston, TX 77036, and was unable to identify a business by the name of Donald Candy Shop at the address. According to USPS databases, 21441 Carrington Road, Houston, TX 77036 is not a valid address.

45. Your Affiant knows based on training and experience, that individuals using the U. S. Mails for the purpose of transporting controlled substances will often place fictitious address and/or name information, different variations of their names, or no names at all on these parcels, to conceal their true identities from law enforcement should the parcel be seized.

46. On November 16, 2018, the Target Parcel was placed into a lineup containing several blank parcels which emanated no narcotics odors. Narcotic detection canine "Jimmy," handled by Detective Anthony Quirino of the Cuyahoga County Sheriff's Office was allowed to examine the lineup. According to Detective Quirino, Jimmy gave a positive alert on the Target Parcel and none of the blank parcels. According to Detective Quirino, this positive alert meant Jimmy detected the odor of an illegal drug emanating from the Target Parcel.

47. Your Affiant knows based on training and experience that individuals who regularly handle controlled substances often leave the scent of controlled substances, which narcotic canines are trained to indicate alert, on the box, contents of the box, and/or other packaging material they handle.

48. On November 16, 2018, in the Northern District of Ohio, Eastern Division, your Affiant applied for and was granted a federal search warrant by the Honorable

Magistrate Judge Jonathan D. Greenberg, authorizing the search of the Target Parcel. Postal Inspectors executed a search of the Target Parcel on this day and identified approximately 100 blue round tablets each marked with the imprint "A 215" in a clear baggie and concealed in a Quaker State oatmeal packet. The aggregate weight of the baggie containing the tablets was approximately 13 grams.

49. Based on training and experience, your Affiant knows that blue round tablets with the marking "A 215" can actually be Oxycodone Hydrochloride 30 milligram, a Schedule II controlled substance, manufactured by legitimate pharmaceutical companies. On the other hand, also based on training and experience, your Affiant also knows that blue round tablets pressed with Fentanyl or Carfentanil are often sold on the dark web marketplace and disguised as Oxycodone Hydrochloride 30 milligram by the sellers in attempt to thwart law enforcement detection.

50. Your Affiant examined USPS business records and identified a history of similar USPS parcels from the Houston, Texas, area delivered to the Target Location. On May 30, 2018, a USPS Priority Mail Flat Rate Envelope addressed to Steve Chase, with a return address of Sims Candy Shop, 1442 Roadrunner Lane, Humble, TX 77396 was delivered to the Target Location. On May 12, 2018, a USPS Priority Mail Flat Rate Envelope addressed to Steve Chase, with a return address of Donald Candy Shop, 4211 Wilshire Road, Houston, TX 77036 was delivered to the Target Location. On March 14, 2018, a USPS Priority Mail Flat Rate Envelope addressed to Mr. Steve Chase, with a return address of Chris Johnson, 6001 Reims Rd, Houston, TX 77036 was delivered to the Target Location.

51. Affiant avers that on November 19, 2018, the blue tablets marked "A215"

were submitted to the Cuyahoga County Regional Forensic Laboratory ("CCRFSL") for chemistry examination. The CCRFSL issued a laboratory report on November 19, 2018, stating there were approximately 97 blue round pills in the clear plastic bag. The CCRFSL identified the presence of Carfentanil in the blue round pills, with a net weight of approximately 12.66 grams. I know from training and experience, this amount of Carfentanil is a distribution amount, not a personal use amount.

52. Based on the foregoing, your Affiant suspects that the blue round tablets seized from the Target Parcel marked as "A 215" were intentionally disguised by the seller to appear as Oxycodone Hydrochloride 30 milligram to thwart law enforcement detection.

53. On November 19, 2018, members of the USPIS and Cleveland Police Department Narcotics (CPD) conducted a controlled delivery of the Target Parcel to the stated delivery address. Prior to the controlled delivery, agents removed all of the Carfentanil pills from the Target Parcel and replaced the pills with a sham substance. Inspectors also equipped the package with an electronic tracking device and a sensor that would alert investigators when the package was opened. At approximately 12:18 p.m., an undercover Inspector acting as a USPS letter carrier, delivered the Target Parcel by placing it on top of the designated mailbox, which was next to the front door of the delivery address located at 730 E 101st St. The delivery addresses of 730, 728, 726, and 724 E 101st St are all located in the same residential structure and share a common front porch.

54. At approximately 12:32 p.m., officers observed an unknown African-American male exit the front door of 724 E 101st St, Cleveland, OH, three doors down from the delivery address, walk down to 730 E 101st St and retrieve the Target Parcel from on top of the mailbox. Then male then brought the Target Parcel into the residence located at 724

E 101st St.

55. According to CLEAR and the Ohio Law Enforcement Gateway, Courtney Johnson, an African-American male, was associated with 724 E 101st St, Cleveland, OH 44108. Officers identified Johnson as the person who retrieved the Target Parcel from the mailbox. According to CLEAR, an African-American male by the name of Elliet Lanier was formerly associated with 724 E 101st St, Cleveland, OH 44108.

56. At approximately 2:36 p.m., a black Chrysler minivan bearing Arizona license plate CBV 6647, registered to E Lanier, 3030 E 63rd St Apt 311, Cleveland, OH, arrived at E 101st St from St. Clair Ave and parked in front of 730 E 101st St. At approximately 2:40 p.m., Johnson exited 724 E 101st St with the Target Parcel and approached the black minivan. Johnson handed the Target Parcel through the driver side window of the minivan and then conversed with the driver of the minivan for several minutes. Johnson then entered the front passenger side of the minivan. At approximately 3:00 p.m., Johnson exited the passenger side of the minivan and the minivan, departed E 101st St. Officers observed the driver of the minivan and confirmed it was the registered owner, E. (Elliet) Lanier, based on his Ohio Driver's License photograph.

57. From approximately 3:00 p.m. through 9:40 p.m., officers conducted surveillance of the minivan and observed Lanier stop at several locations in Cleveland, Ohio, and the greater Cleveland area. The Target Parcel never left the minivan during the stops.

58. At approximately 9:40 p.m., Lanier pulled into the driveway of the residence located at 3560 E 144th St, Cleveland, OH 44120 and parked the minivan next to the side door of the residence. According to CLEAR, this was a former address associated with Lanier. Officers parked behind the minivan in the driveway and called Lanier out of the

driver side of the minivan. Lanier was detained without incident. Your Affiant recovered a Samsung cellular phone from Lanier's hand as he was taken into custody. Officers also recovered a loaded Smith & Wesson M&P .45 caliber handgun from Lanier's person. Lanier had a Cuyahoga County Ohio License to Carry a Concealed Handgun in his wallet.

59. Officers recovered the Target Parcel from behind the center console of the minivan. The Target Parcel was unopened. In addition to the Target Parcel, officers also recovered a black notebook. Within the notebook were handwritten notes pertaining to bitcoin wallets and transactions. One page of the notebook in particular had the heading, "Electronic Currency," with the words "bitcoin, monero, ethereum, and ripple written under it." Other pages in the notebook contained handwritten authorization keys and usernames for digital currency and bitcoin wallet accounts. The following accounts were identified in the black notebook:

a. The Bitstamp.net on-line bitcoin exchange account associated with the email stevechase2015@protonmail.com, client ID number 268962, or username Lanierlife9816,

b. The hitbtc.com on-line digital currency exchange account associated with the email lanierlife@gmail.com,

c. The paragoncoin.com on-line digital currency exchange account associated with the email lanierlife@gmail.com,

d. The gatehub.net on-line digital currency exchange account associated with the email lanierlife@gmail.com,

e. The bittrex.com on-line digital currency exchange account associated with

the email lanierlife@gmail.com,

60. Your Affiant believes that the tablets containing Carfentanil inside the Target Parcel were ordered from the dark web using digital currency. Based on the handwritten notes in the ledger, your Affiant believes Lanier had the knowledge and means to purchase Carfentanil or other controlled substances from the dark net marketplace using digital currency.

61. Officers explained to Lanier the reason why he was detained. Lanier stated he did not know what was in the Target Parcel. Lanier told officers he resided at 3560 E 144th St in the basement. Officers made contact with Lanier's sister, Lori Lanier-Robinson, who exited the residence to speak with officers. Lanier-Robinson stated she was the owner of the residence located at 3560 E 144th St. Lanier-Robinson advised officers that Lanier pays rent for an upstairs bedroom and for a room in the basement. Lanier initially provided verbal consent for officers to search the basement, but retracted consent after officers learned he also had an upstairs bedroom.

62. Lanier-Robinson advised officers she had AT&T U-Verse internet established at her residence. It should be noted that an Internet Protocol ("IP") address associated with AT&T U-Verse in Cleveland, Ohio, was used to track the delivery status of the Target Parcel several times using USPS.com and/or a USPS application. Based on the foregoing, your Affiant has reason to believe that the IP address associated with the AT&T U-Verse internet account at 3560 E 144th St was used to track the delivery status of the Target Parcel.

63. During the early hours of November 20, 2018, officers obtained a Cuyahoga County search warrant for the residence located at 3560 E 144th St, Cleveland, OH 44120.

Officers recovered evidence of drug manufacturing and distribution from Lanier's upstairs bedroom, including unknown powdery substances knotted in clear zip lock bags and a silver mylar bag, clear zip lock bags of various sizes, small white pouches, mixing utensils, 3M ventilation masks, and two digital scales. Based on your Affiant's training and experience, the aforementioned items are commonly associated with the distribution of Fentanyl and Carfentanil.

64. On November 21, 2018, your Affiant submitted six different items to the CCRFSL for chemistry examination. Each of the items contained powdery substances recovered from Lanier's upstairs bedroom. The CCRFSL examined the substances and confirmed each of the substances contained a mixture of Heroin, a Schedule I controlled substance, Fentanyl, a Schedule II controlled substance, and 4-ANPP, a Schedule II controlled substance. The net weight of the substances containing Heroin, Fentanyl, and 4-ANPP was approximately 37.87 grams.

65. Officers recovered five cellular phones, an Apple iPad, HP laptop, HP personal computer, and three electronic storage devices Lanier's residence. Officers also recovered a brown portfolio in the basement located near the HP laptop computer. The brown portfolio contained bills and other mailed correspondence addressed to E Lanier.

66. Within the brown portfolio, your Affiant found documents listing usernames and passwords for on-line dark net marketplace accounts known to sell controlled substances, digital currency exchange accounts, such as on-line sites to purchase bitcoin, and digital currency wallets where bitcoin and other digital currency can be transferred to other digital currency wallets. Your Affiant identified the following accounts, usernames, and passwords from the documents recovered from the brown portfolio:

a. User account “gregorian45” that is stored on the server hosting Tor hidden service Dream Market, a dark net marketplace identified by the Tor URL http://uhivlt5grrqjhad7.onion/?ai=1675,

b. User account “gregorian45” that is stored on the server hosting Tor hidden service Wall Street Market, a dark net marketplace identify by the Tor URL http://wallst4qihu6lvsa.onion/signup?ref=276,

c. User account “steve1” that is stored on the server hosting Tor hidden service Point / T CHKA Free Market, a dark net marketplace identified by the Tor URL http://pointgg344ghbo2s.onion/auth/register/563636d36ab740e4720f44e8328441d3

d. The Coincure.net bitcoin wallet account associated with the email stevechase2015@protonmail.com or username “stevehase0702”,

e. The Electrum.org bitcoin wallet account associated with the email stevechase2015@protonmail.com,

f. The Bitstamp.net on-line bitcoin exchange account associated with the email stevechase2015@protonmail.com, client ID number 268962, or username Lanierlife9816,

g. The localbitcoins.com on-line bitcoin exchange account associated with the username “davenport216” or email davenport1522@mail.com,

h. The binance.com on-line bitcoin exchange account associated with the username “lanierlife” or email lanierlife@gmail.com,

i. The liqui.io on-line digital currency exchange account associated with the username “lanierlife” or email lanierlife@gmail.com,

67. The email address associated with the Coincure, Electrum, and BitStamp accounts was stevechase2015@protonmail.com. The Target Parcel containing tablets containing Carfentanil was addressed to Steve Chase.

68. Agents have continued searching through the documents seized from Lanier. During the search, they uncovered notations indicating the username, password, and other recovery methods for the **Target Accounts.** The administrators of the dark net marketplace accounts (Dream Market, Wall Street Market, and Point / T CHKA Free Market) purposely conceal the location of their servers (and thus the data relating to the **Target Accounts**), making it infeasible for law enforcement to shut down the site at this time. Based on your Affiant's training and experience, the **Target Accounts** contain vital information relating to this investigation, including detailed information regarding past and pending drug sales. Law enforcement now seeks authority from this Court to access the **Target Accounts** and seize the items described in Attachment B.

THE REMOTE SEARCH TECHNIQUE

69. Based on my training, experience, and the investigation described above, I have concluded that using a remote search technique may help investigative agents locate additional evidence of Elliet Lanier's criminal activity and identify additional information and evidence pertaining to the purchase and distribution of illegal narcotics. Accordingly, I request authority to use the remote search technique to investigate the **Target Accounts.**

70. The remote search of the accounts will entail an investigative agent logging into the accounts and checking the account profile, the account transaction logs, and other portions of the account that may contain records related to the purchase and sale of illegal narcotics. An investigative agent will use the **Target Accounts'** account information to log into the sites from

a covert Internet connection. The agent will take steps to save the webpages as individual files and/or take screenshots of the specific pages. The agent will not make any changes to the account.

71. Each of these categories of information described in Attachment B may constitute evidence of the crimes under investigation, showing a direct link and profit from the sale of illegal narcotics.

72. It is further requested that the Court authorize execution of the warrant at any time of day or night, as the warrant does not authorize the physical seizure of tangible property.

CONCLUSION

73. Based on the information contained herein, your Affiant maintains there is probable cause to believe that the **Target Accounts** further described in Attachment A contain evidence establishing violations of the aforementioned federal laws. Your Affiant seeks permission to search the **Target Accounts** for evidence described in Attachment B.

I, Postal Inspector Marc Kudley, being duly sworn according to law, deposes, and states that the facts stated in the foregoing Affidavit are true and correct to the best of his knowledge, information, and belief

MARC A. KUDLEY
U.S. POSTAL INSPECTOR

This affidavit was sworn to by the affiant, who did no more than attest to its contents pursuant to Crim. R. 4.1 (b)(2)(A), by telephone after a PDF was transmitted by email, per Crim R. 4.1 THIS 28th DAY OF NOVEMBER, 2018

WILLIAM H. BAUGHMAN, JR.
U. S. MAGISTRATE JUDGE